VECTRA

DATA SHEET

Vectra AI Platform Azure AD and M365 metadata attributes and descriptions

This document describes the important attributes in all the Azure AD & M365 metadata streams supported by Vectra AI Platform.

Audit Azure Active Directory	
Field	**Description**
actor_context_id	The GUID of the organization that the actor belongs to
actor_ip_address	The actor's IP address in IPV4 or IPV6 address format
actor.0.id	The value of the identity given the type
actor.0.type	The type of the identity
application_id	The ID of application that triggers the account login event, such as Office 15
azure_active_directory_event_type	The type of Azure AD event
client_id	Details about the client device, device OS, and device browser that was used for the of the account login event
client_ip	The IP address of the device that was used when the activity was logged
creation_time	The date and time in Coordinated Universal Time (UTC) when the user performed the activity
device_properties_display_name	Human-readable device name (e.g. name of the Windows instance, name of mobile device, etc.)
device_properties.0.name	The name of the device property. This property includes various device details, including Id, Display name, OS, Browser, IsCompliant, IsCompliantAndManaged, SessionId, and DeviceTrustType
device_properties.0.value	The value of the device property
error_number	For failed logins (where the value for the Operation property is UserLoginFailed), this property contains the Azure Active Directory STS (AADSTS) error code
extended_properties_audit_event_category	Extended property parameter
extended_properties_result_status_detail	For sign-in operations - an indicator of whether operation completed or resulted in a redirect

Audit Azure Active Directory	
Field	**Description**
extended_properties_result_type	Extended property parameter
extended_properties_target_upn	Extended property parameter
extended_properties_user_agent	Browser user agent string
extended_properties_user_authentication_method	Authentication method ID (not mandatory)
extended_properties.0.name	The name of the extended properties of the Azure AD event
extended_properties.0.value	The value of the extended properties of the Azure AD event
id	Unique ID representing the activity
inter_systems_id	The GUID that track the actions across components within the Office 365 service
intra_systems_id	The GUID that's generated by Azure Active Directory to track the action
logon_error	For failed logins, this property contains a user-readable description of the reason for the failed login
modified_properties.0.display_name	Name of the modified property
modified_properties.0.new_value	New value of the modified property
modified_properties.0.old_value	Old value of the modified property

Audit Azure Active Directory	
Field	**Description**
object_id	For SharePoint and OneDrive for Business activity, the full path name of the file or folder accessed by the user
operation	The name of the operation
organization_id	The GUID for your organization's tenant
record_type	The type of operation indicated by the record
result_status	Operation result
support_ticket_id	The customer support ticket ID for the action in "act-on-behalf-of" situations.
target_context_id	The GUID of the organization that the targeted user belongs to
target.0.id	The id of user that the action (identified by the Operation property) was performed on
target.0.type	The identity type of the user that the action (identified by the Operation property) was performed on
timestamp	Event timestamp
user_domain	The Tenant Identity Information (TII)
user_id	The UPN (User Principal Name) of the user who performed the action (specified in the Operation property) that resulted in the record being logged; for example, my_name@my_domain_name
user_key	An alternative ID for the user identified in the UserId property
user_type	The type of user that performed the operation
vectra.identity_principal	Vectra field that identifies the user performing the action
workload	The service where the activity occurred

Audit Exchange	
Field	**Description**
client_app_id	The Id of the AAD app that performed the access on behalf of the user
client_info_string	Information about the email client that was used to perform the operation, such as a browser version, Outlook version, and mobile device information
client_ip	The IP address of the device that was used when the activity was logged
client_ip_address	The IP address of the device that was used when the operation was logged
client_ip.usage	The IP address of the device that was used when the activity was logged
client_machine_name	The machine name that hosts the Outlook client
client_process_name	The email client that was used to access the mailbox
client_version	The version of the email client
creation_time	The date and time in Coordinated Universal Time (UTC) when the user performed the activity
external_access	Specifies whether the cmdlet was run by a user in your organization, by Microsoft datacenter personnel or a datacenter service account, or by a delegated administrator
folder.Id	The store ID of the folder object
folder.Path	The name of the mailbox folder where the message that was accessed is located
id	Unique identifier of an audit record
internal_logon_type	Reserved for internal use (Owner, Admin, etc)
item_flat	Represents the item upon which the operation was performed
logon_type	Indicates the type of user who accessed the mailbox and performed the operation that was logged
logon_user_display_name	The user-friendly name of the user who performed the operation
logon_user_sid	The SID of the user who performed the operation

Audit Exchange	
Field	**Description**
mailbox_guid	The Exchange GUID of the mailbox that was accessed
mailbox_master_account_sid	The SID of the mailbox owner
mailbox_owner_sid	The SID of the mailbox owner
mailbox_owner_upn	The email address of the person who owns the mailbox that was accessed
modified_object_resolved_name	This is the user friendly name of the object that was modified by the cmdlet
modified_properties.0	The property is included for admin events. The property includes the name of the property that was modified, the new value of the modified property, and the previous value of the modified object
object_id	The name of the object that was modified by the cmdlet
operation	The name of the user or admin activity
operation_properties.0.name	Name of the extra property (Extra properties, i.e. number of OTP passcode sent, email subject, etc.)
operation_properties.0.value	Value of the extra property
organization_id	The GUID for your organization's Office 365 tenant
organization_name	The name of the tenant
originating_server	The name of the server from which the cmdlet was executed
parameters.0.name	The name for a parameter that was used with the cmdlet that is identified in the Operations property
parameters.0.value	The value for a parameter that was used with the cmdlet that is identified in the Operations property
record_type	The type of operation indicated by the record
result_status	Indicates whether the action (specified in the Operation property) was successful or not
timestamp	Event timestamp

Audit Exchange	
Field	**Description**
user_id	The UPN (User Principal Name) of the user who performed the action (specified in the Operation property) that resulted in the record being logged; for example, my_name@my_domain_name
user_key	An alternative ID for the user identified in the UserId property. This property is populated with the passport unique ID (PUID) for events performed by users in SharePoint, OneDrive for Business, and Exchange
user_type	The type of user that performed the operation
vectra.identity_principal	Vectra field that identifies the user performing the action
workload	The Office 365 service where the activity occurred

Audit General	
Field	**Description**
add_on_name	The name of the add-on that generated the event
attachment_data.0.file_verdict	The file malware verdict
attachment_data.0.filename	The file name of the attachment
attachment_data.0.filetype	The file type of the attachment
attachment_data.0.malware_family	The file malware family
attachment_data.0.sha256	The file SHA256 hash
case_id	eDiscovery case ID
client_ip	The IP address of the device that was used when the activity was logged
communication_type	Type of communication (e.g. Team, Group Chat, Meeting, etc)
creation_time	The date and time in Coordinated Universal Time (UTC) when the user performed the activity
detection_method	The method or technology used by Defender for Office 365 for the detection

Audit General	
Field	**Description**
exchange_locations	Exchange mailbox locations covered in eDiscovery operations
extended_properties.0.name	Extended properties related to the logged operation
extended_properties.0.value	Extended properties related to the logged operation
flow_connector_names	PowerAutomate Flow names
flow_details_url	PowerAutomate Flow URL
id	Unique identifier of an audit record
item_name	Item name (meaning is operation-specific)
members.0.display_name	Team member display name
members.0.role	Team member role
members.0.upn	Team member unique name
name	Name parameter (operation-specific)
object_id	For SharePoint and OneDrive for Business activity, the full path name of the file or folder accessed by the user
operation	The name of the user or admin activity
organization_id	The GUID for your organization's Office 365 tenant
p1_sender	The return path of sender of the email message
p2_sender	The from sender of the email message
parameters	Operation parameters
policy	The type of filtering policy (for example Anti-spam or Anti-phish) and related action type (such as High Confidence Spam, Spam, or Phish) relevant to the email message
query	The query that was used to identify the messages of the mail cluster
query_id	eDiscovery query ID
query_text	eDiscovery text
recipients.0	An array of recipients of the email message
record_type	The type of operation indicated by the record
result_status	Indicates whether the action (specified in the Operation property) was successful or not
sources.0.created_by	Parameters for eDiscovery operations

Audit General	
Field	**Description**
sources.0.created_by_id_set	Parameter for eDiscovery operations
sources.0.created_by_id_set_v2.user.display_name	Parameter for eDiscovery operations
sources.0.created_by_id_set_v2.user.id	Parameter for eDiscovery operations
sources.0.creation_date_time.date_time	Parameter for eDiscovery operations
sources.0.creation_date_time.offset_minutes	Parameter for eDiscovery operations
sources.0.deleted_by	Parameter for eDiscovery operations
sources.0.deletion_date_time	Parameter for eDiscovery operations
sources.0.display_name	Parameter for eDiscovery operations
sources.0.graph_or_email_id	Parameter for eDiscovery operations
sources.0.is_disabled_for_search	Parameter for eDiscovery operations
sources.0.last_modification_date_time.date_time	Parameter for eDiscovery operations
sources.0.last_modification_date_time.offset_minutes	Parameter for eDiscovery operations
sources.0.last_modified_by	Parameter for eDiscovery operations
sources.0.location	Parameter for eDiscovery operations
sources.0.on_hold	Parameter for eDiscovery operations
sources.0.query_scope	Parameter for eDiscovery operations
sources.0.source_category	Parameter for eDiscovery operations
sources.0.source_id	Parameter for eDiscovery operations
sources.0.sub_locations	Parameter for eDiscovery operations
sources.0.use_location_as_is	Parameter for eDiscovery operations
sources.0.workload	Parameter for eDiscovery operations
subject	The text in the Subject field of the email message
team_guid	A unique identifier for the team being audited
team_name	The name of the team being audited

Audit General	
Field	**Description**
timestamp	Event timestamp
user_agent	User-Agent header of the client application
user_id	The UPN (User Principal Name) of the user who performed the action (specified in the Operation property) that resulted in the record being logged; for example, my_name@my_domain_name
user_key	An alternative ID for the user identified in the UserId property
user_type	The type of user that performed the operation
vectra.identity_principal	Vectra field that identifies the user performing the action
verdict	The message verdict
workload	The Office 365 service where the activity occurred

Audit Sharepoint	
Field	**Description**
client_ip	The IP address of the device that was used when the activity was logged
correlation_id	An identifier that can be used to correlate a specific user's actions across Microsoft 365 services
creation_time	The date and time in Coordinated Universal Time (UTC) when the user performed the activity
custom_event	Optional string for custom events
destination_file_extension	The file extension of a file that is copied or moved. This property is displayed only for the FileCopied and FileMoved user activities
destination_file_name	The name of the file is copied or moved. This property is displayed only for the FileCopied and FileMoved actions
destination_relative_url	The URL of the destination folder where a file is copied or moved
event_source	Identifies that an event occurred in SharePoint

Audit Sharepoint	
Field	**Description**
file_sync_bytes_committed	Number of bytes transferred in file upload/download operation
id	The ID of the report entry
item_type	The type of object that was accessed or modified
list_id	The Guid of the list. This information is present only if it is applicable
list_item_unique_id	The Guid of uniquely an identifiable item of list. This information is present only if it is applicable
machine_domain_info	Information about device sync operations
machine_id	Information about device sync operations
object_id	For SharePoint and OneDrive for Business activity, the full path name of the file or folder accessed by the user
operation	The name of the user or admin activity
organization_id	The GUID for your organization's Office 365 tenant
record_type	The type of operation indicated by the record
sharing_type	The type of sharing permissions that was assigned to the user that the resource was shared with
site	The GUID of the site where the file or folder accessed by the user is located
site_url	The URL of the site where the file or folder accessed by the user is located
source_file_extension	The file extension of the file that was accessed by the user. This property is blank if the object that was accessed is a folder
source_file_name	The name of the file or folder accessed by the user
source_name	The entity that triggered the audited operation
source_relative_url	The URL of the folder that contains the file accessed by the user
target_user_or_group_name	Stores the UPN or name of the target user or group that a resource was shared with

Audit Sharepoint	
Field	**Description**
target_user_or_group_type	Identifies whether the target user or group is a Member, Guest, Group, or Partner
timestamp	Event timestamp
user_agent	Information about the user's client or browser
user_id	The UPN (User Principal Name) of the user who performed the action (specified in the Operation property) that resulted in the record being logged; for example, my_name@my_domain_name
user_key	An alternative ID for the user identified in the UserId property. This property is populated with the passport unique ID (PUID) for events performed by users in SharePoint, OneDrive for Business, and Exchange
user_shared_with	The user that a resource was shared with
user_type	The type of user that performed the operation
vectra.identity_principal	Vectra field that identifies the user performing the action
workload	The Office 365 service where the activity occurred

Directory Audits	
Field	**Description**
activity_date_time	Indicates the date and time the activity was performed
activity_display_name	Indicates the activity name or the operation name (examples: "Create User" and "Add member to group").
additional_details.0.key	Key for the key-value pair
additional_details.0.value	Value for the key-value pair
category	Indicates which resource category that's targeted by the activity. (For example: User Management, Group Management etc..)
	Physical Port Number of the Device Authenticating the User
client_ip	The IP address of the device that was used when the activity was logged
correlation_id	Indicates a unique ID that helps correlate activities that span across various services. Can be used to trace logs across services
creation_time	Indicates the date and time the activity was performed
id	Indicates the unique ID for the activity. This is a GUID
initiated_by.app.app_id	Refers to the Unique GUID representing Application Id in the Azure Active Directory
initiated_by.app.display_name	Refers to the Application Name displayed in the Azure Portal
initiated_by.app.service_principal_id	Refers to the Unique GUID indicating Service Principal Id in Azure Active Directory for the corresponding App
initiated_by.app.service_principal_name	Refers to the Service Principal Name is the Application name in the `tenant
	This is the maximum session length
initiated_by.user.display_name	The identity's display name. Note that this may not always be available or up-to-date
initiated_by.user.id	Unique identifier for the identity
initiated_by.user.ip_address	Indicates the client IP address used by user performing the activity
initiated_by.user.user_principal_name	The userPrincipalName attribute of the user
logged_by_service	Indicates information on which service initiated the activity
operation_type	Indicates the type of operation that was performed

Directory Audits	
Field	**Description**
result	Indicates the result of the activity
result_reason	Indicates the reason for failure if the result is failure or timeout
target_resources.0.display_name	Indicates the visible name defined for the resource. Typically specified when the resource is created
target_resources.0.group_type	When type is set to Group, this indicates the group type
target_resources.0.id	Indicates the unique ID of the resource
target_resources.0.modified_properties.0.display_name	Indicates the property name of the target attribute that was changed
target_resources.0.modified_properties.0.new_value	Indicates the updated value for the property
target_resources.0.modified_properties.0.old_value	Indicates the previous value (before the update) for the property
target_resources.0.type	Describes the resource type
target_resources.0.user_principal_name	When type is set to User, this includes the user name that initiated the action; null for other types
timestamp	Event timestamp
vectra.identity_principal	Vectra field that identifies the user performing the action

SignIns	
Field	**Description**
app_display_name	App name displayed in the Azure Portal
app_id	Unique GUID representing the app ID in the Azure Active Directory
applied_conditional_access_policies.0.display_name	Refers to the Name of the conditional access policy (example: “Require MFA for Salesforce”)
applied_conditional_access_policies.0.enforced_grant_controls.0	Refers to the grant controls enforced by the conditional access policy (example: “Require multi-factor authentication”)
applied_conditional_access_policies.0.enforced_session_controls.0	Refers to the session controls enforced by the conditional access policy (example: “Require app enforced controls”)
applied_conditional_access_policies.0.id	An identifier of the conditional access policy
applied_conditional_access_policies.0.result	Indicates the result of the CA policy that was triggered
client_app_used	Identifies the client used for the sign-in activity
client_ip	The IP address of the device that was used when the activity was logged
conditional_access_status	Reports status of an activated conditional access policy
correlation_id	The request ID sent from the client when the sign-in is initiated; used to troubleshoot sign-in activity
created_date_type	Date and time (UTC) the sign-in was initiated
creation_time	Indicates the date and time the activity was performed
device_detail.browser	Indicates the browser information of the used for signing in
device_detail.device_id	Refers to the UniqueID of the device used for signing in
device_detail.display_name	Refers to the name of the device used for signing in
device_detail.is_compliant	Indicates whether the device is compliant
device_detail.is_managed	Indicates whether the device is managed
device_detail.operating_system	Indicates the operating system name and version used for signing in

SignIns	
Field	**Description**
device_detail.trust_type	Provides information about whether the signed-in device is Workplace Joined, AzureAD Joined, Domain Joined
id	Unique ID representing the sign-in activity
ip_address	IP address of the client used to sign in
is_interactive	Indicates if a sign-in is interactive or not
location.city	Provides the city where the sign-in originated. This is calculated using latitude/longitude information from the sign-in activity
location.country_or_region	Provides the country code info (2 letter code) where the sign-in originated. This is calculated using latitude/longitude information from the sign-in activity
location.geo_coordinates. altitude	The altitude (height), in feet, above sea level for the item
location.geo_coordinates. latitude	The latitude, in decimal, for the item
location.geo_coordinates. longitude	The longitude, in decimal, for the item
location.state	Provides the State where the sign-in originated
resource_display_name	Name of the resource the user signed into
resource_id	ID of the resource that the user signed into
risk_detail	Provides the 'reason' behind a specific state of a risky user, sign-in or a risk event
risk_event_types_v2.0	A risk event type associated with the sign-in
risk_event_types.0	A risk event type associated with the sign-in
risk_level_aggregated	Aggregated risk level
risk_level_during_sign_in	Risk level during sign-in
risk_state	Reports status of the risky user, sign-in, or a risk event
status.additional_details	Provides additional details on the sign-in activity
status.error_code	Provides the 5-6 digit error code that's generated during a sign-in failure
status.failure_reason	Provides the error message or the reason for failure for the corresponding sign-in activity
timestamp	Event timestamp

SignIns	
Field	**Description**
user_display_name	Display name of the user that initiated the sign-in
user_id	ID of the user that initiated the sign-in
user_principal_name	User principal name of the user that initiated the sign-in
vectra.identity_principal	Vectra field that identifies the user performing the action

For more information about Vectra AI metadata attributes, please contact a service representative or email us at info@vectra.ai.

Email info@vectra.ai vectra.ai